Robustness of LLM-Based Recommendation Agents to Noisy and Adversarial Review Data

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 15 peer-reviewed papers addressing the following research question: How robust are LLM-based recommendation agents to noisy or adversarial review data when evaluated on cross-domain benchmarks like HUMAN-EVAL-R for code generation. Current evaluation frameworks and benchmarks for LLM powered agents focus on text chat driven agents, these frameworks do not expose the persona of user to the agent, thus operating in a user agnostic environment. Importantly, in customer experience management domain, the. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 2.3/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: MM-tau-p^2: Persona-Adaptive Prompting for Robust Multi-Modal Agent Evaluation in Dual-Control Settings. Research question: How robust are LLM-based recommendation agents to noisy or adversarial review data when evaluated on cross-domain benchmarks like HUMAN-EVAL-R for code generation?.

2 Methodology

Systematic literature search across multiple databases yielded 15 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 2.3/10.

3 Results

15 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 2.3/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

References

- http://arxiv.org/abs/2603.09643v5
- http://arxiv.org/abs/2511.00176v1
- http://arxiv.org/abs/2509.12382v1